



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/622,371	02/16/2001	Kunihiko Miyazaki	ASA-907	3509

24956 7590 03/10/2004

MATTINGLY, STANGER & MALUR, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER

NGUYEN, MINH DIEU T

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 03/10/2004

8

Please find below and/or attached an Office communication concerning this application or proceeding.

84

Office Action Summary

Application No.

09/622,371

Applicant(s)

MIYAZAKI ET AL.

Examiner

Minh Dieu Nguyen

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-9 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1, 2, 4, 6, 7 and 9 is/are rejected.
- 7) ☒ Claim(s) 3, 5 and 8 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: ____.

DETAILED ACTION

1. Claims 1-9 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a) As to claims 1 and 6, the phrase "well-known processing method" is indefinite; the phrase "processing apparatus of the secret information is constructed" and the phrase "without allowing said secret information to appear in said arithmetic operation processing circuit, said storing circuit, and said signal line" seem contradict with each other.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. **Claims 1, 2, 4, 6-7 and 9** are rejected under 35 U.S.C. 102(b) as being anticipated by Ishii (5,768,389).

a) **As to claims 1 and 6**, as best understood, Ishii discloses a method and a system for generation and management of a secret key of a public key cryptosystem, such that a secret key can be kept in secret from everyone. The personal portable device (Figure 14, element 34) which reads on a processing apparatus consists of a cipher key generation program unit which reads on an arithmetic operation processing circuit (Figure 14, element 44); storage units (Figure 14, elements 45 and 46) and a signal line connecting them. The system is constructed to possibly reproduce the secret key stored in a personal portable device so as to obtain a same processing result as a processing result obtained by processing the secret information and data as a processing target (Figures 17-21). The storing unit holds reproduced secret key which reads on the secret information forming information that is different from the secret key which reads on the secret information (col. 24, lines 26-67 – col. 25, lines 1-6). The secret information forming information processing means for outputting the processing result by using the reproduced secret key and the data serving as a processing target without allowing the secret information to be read out (col. 24, lines 9-22) which reads on not allowing the secret information to appear in the arithmetic operation processing circuit, the storing circuit and the signal line. The arithmetic operation processing circuit executes the reproduced secret key (Figure 14).

- b) **As to claims 2 and 7**, as best understood, Ishii discloses a system wherein the storing circuit holds the secret information forming information as a plurality of secret information partial information (col. 24, lines 44-46; lines 65-67 – col. 25, lines 1-6).
- c) **As to claim 4**, as best understood, Ishii discloses a system wherein the secret information is a private key for decrypting or forming a digital signature in a public key encryption technique (col. 1, lines 47-51).
- d) **As to claim 9**, as best understood, Ishii discloses a processing system of secret information for transmitting and receiving the processing result by using the secret information by using a processing apparatus (Figure 17, element 55) of secret information wherein an apparatus on a receiver side of the processing result has means for setting the secret information forming information processing means and the secret information forming information into the storing circuit of the processing apparatus (col. 23, lines 5-67 – col. 24, lines 1-22) and an apparatus on a user side of the processing apparatus comprises means for inputting the data serving as a processing target to the processing apparatus, means for receiving the processing result from the processing apparatus and means for transmitting the received processing result to the receiver side apparatus (Figure 17-19).

Allowable Subject Matter

6. Claims 3, 5 and 8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure

- a) Methods and Apparatus for Verifying the Cryptographic Security of a Selected Private and Public Key Pair Without Knowing the Private Key, Liskov et al. (6,411,715).
- b) Two Phase Cryptographic Key Recovery System, Gennaro et al., (5,937,066).
- c) Multi Step Digital Signature Method and System, Sudia et al., (5,825,880).

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 703-305-9727. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789.

The fax phone numbers for the organization where this application or proceeding is assigned are:

703-746-7238	for After-Final communications
703-872-9306	for Official communications
703-746-5661	for Non-Official/Draft communications

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

mdn
Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
3/2/04

Gregory Morse
GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100